AF

JPW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Kevin R. Driscoll	Examiner:	Jenise E. Jackson
Serial No.:	09/712,505	Group Art Unit:	2131
Filed:	November 14, 2000	Docket No.:	H16-26353 (H162.104.101)
Date Due:	September 1, 2005		
Title:	CRYPTOGRAPHIC COMBINER USING TWO SEQUENTIAL NON-ASSOCIATIVE OPERATIONS		

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

We are transmitting herewith the attached:

☒ Transmittal Sheet containing Certificate of Mailing (1 pg.).

☒ Appeal Brief under 37 C.F.R. § 41.37 (17 pgs.).

☒ Authorization to charge Deposit Account 500471 in the amount of $500.00 for filing a Brief in Support of an Appeal as set forth under 37 C.F.R. § 41.20(b)(2).

☒ Return Postcard.

Please consider this a PETITION FOR EXTENSION OF TIME for a sufficient number of months to enter these papers, if appropriate. At any time during the pendency of this application, please charge any additional fees or credit overpayment to Deposit Account No. 500471.

By: _____
Name: Patrick G. Billig
Reg. No.: 38,080

HONEYWELL INTERNATIONAL, INC.
Law Department AB2
P.O. Box 2245
Morristown, New Jersey 07962-9806

CERTIFICATE UNDER 37 C.F.R. 1.8: The undersigned hereby certifies that this paper or papers, as described herein, are being deposited in the United States Postal Service, as first class mail, in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on this 1 day of September, 2005.

By _____
Name: Patrick G. Billig

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Applicant:	Kevin R. Driscoll	Examiner: Jenise E. Jackson
Serial No.:	09/712,505	Group Art Unit: 2131
Filed:	November 14, 2000	Docket No.: H16-26353 (H162.104.101)
Title:	CRYPTOGRAPHIC COMBINER USING TWO SEQUENTIAL NON-ASSOCIATIVE OPERATIONS	

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

This Appeal Brief is submitted in support of the Notice of Appeal filed on July 1, 2005, appealing the final rejection of claims 1-43 of the above-identified application as set forth in the Final Office Action mailed March 1, 20005.

The U.S. Patent and Trademark Office is hereby authorized to charge Deposit Account No. 500471 in the amount of $500.00 for filing a Brief in Support of an Appeal as set forth under 37 C.F.R. § 41.20(b)(2). At any time during the pendency of this application, please charge any required fees or credit any overpayment to Deposit Account No. 500471.

Appellant respectfully requests consideration and reversal of the Examiner's rejection of pending claims 1-43.

TABLE OF CONTENTS

REAL PARTY IN INTEREST

The real party in interest is Honeywell International, Inc. having a principal place of business at 101 Columbia Road, Morristown, New Jersey 07962-9806.

RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to Appellant that will have a bearing on the Board's decision in the present Appeal.

STATUS OF CLAIMS

In a Final Office Action mailed October 1, 2005, claims 1-43 were finally rejected. The claims were not amended in a Response mailed to the Office on May 2, 2005. Claims 1-43 are pending in the application, and are the subject of the present Appeal.

STATUS OF AMENDMENTS

No amendments have been filed subsequent to the Final Office Action mailed May 2, 2005.

SUMMARY OF THE CLAIMED SUBJECT MATTER

The subject matter of the independent claims involved in the Appeal is related to providing a keystream and cryptographically combining a first binary data sequence and the keystream and performing two sequential non-associative operations on the first binary data sequence and the keystream to provide the second binary data sequence.

One aspect of the present invention, as claimed in independent claim 1, provides a stream cipher cryptosystem (20) including a source (24) for providing an encryption keystream (28). The stream cipher cryptosystem includes an encryption combiner (26) receiving a first plaintext binary data sequence (30) and the encryption keystream and performing a first set of two non-associative operations (126A and 126B) on the first plaintext binary data sequence and the encryption keystream to provide a ciphertext binary data sequence (36). The stream cipher cryptosystem includes a source (44) for providing a decryption keystream (48). The stream

cipher cryptosystem includes a decryption combiner (46) receiving the ciphertext binary data sequence and the decryption keystream and performing a second set of two non-associative operations (146A and 146B) on the ciphertext binary data sequence and the decryption keystream to provide a second plaintext binary data sequence (30') substantially similar to the first plaintext binary data sequence. *See Specification,* at page 6, line 22 through page 12, line 29; and Figures 1 and 2.

Another aspect of the present invention, as claimed in independent claim 9, provides a stream cipher cryptosystem (20) including a source (24 or 44) for receiving a key (32 or 32') and providing a keystream (28 or 48). The stream cipher cryptosystem includes a cryptographic combiner (26 or 46) receiving a first binary data sequence (30 or 36) and the keystream and performing two sequential non-associative operations (126A and 126B, or 146A and 146B) on the first binary data sequence and the keystream to provide a second binary data sequence (36 or 30'). *See Specification*, at page 6, line 22 through page 12, line 29; and Figures 1 and 2.

Another aspect of the present invention, as claimed in independent claim 18, provides a method of encrypting a plaintext binary data sequence (30). The method includes generating an encryption keystream (28) as a function of a key (32). The method includes combining the plaintext binary data sequence and the encryption keystream with two non-associative operations (126A and 126B) to provide a ciphertext binary data sequence (36). *See Specification*, at page 6, line 22 through page 12, line 29; and Figures 1 and 2.

Another aspect of the present invention, as claimed in independent claim 31, provides a method of decrypting a ciphertext binary data sequence (36). The method includes generating a decryption keystream (48) as a function of a key (32'). The method includes combining the ciphertext binary data sequence and the decryption keystream with two non-associative operations (146A and 146B) to provide a plaintext binary data sequence (30'). *See Specification*, at page 6, line 22 through page 12, line 29; and Figures 1 and 2.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

I. Whether claims 1-43 are patentable under 35 U.S.C. § 102(b) over the Ritter U.S. Patent No. 4,979,832.

ARGUMENT

I. The Applicable Law

With regard to a 35 U.S.C. § 102(b) anticipation rejection: "A person shall be entitled to a patent unless- (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of the application for patent in the United States." 35 U.S.C. § 102(b)(2004).

A rejection based on 35 U.S.C. § 102(b) can be overcome by: persuasively arguing that the claims are patentably distinguishable from the prior art; or, amending the claims to patentably distinguish over the prior art. M.P.E.P. § 706.02(b).

II. Rejection of claims 1-43 under 35 U.S.C. § 102(b) as being anticipated by the Ritter U.S. Patent No. 4,979,832.

Claims 1-43 were rejected in the first Office Action mailed July 1, 2004 and in the Final Office Action mailed March 1, 2005 as being anticipated by the Ritter patent. Appellant responded to these rejections in the respective Responses filed October 1, 2004 and May 2, 2005, which include persuasive arguments that claims 1-43 are patentably distinguishable from the Ritter patent.

In particular, independent claims 1, 9, 18, and 31 are patentably distinct from the Ritter patent.

Independent claims 1, 9, 18, and 31 all include limitations related to providing a keystream and cryptographically combining a first binary data sequence and the keystream and performing two sequential non-associative operations on the first binary data sequence and the keystream to provide the second binary data sequence. Independent claim 1 includes both an encryption combiner and a decryption combiner in a stream cipher cryptosystem. Independent claim 9 includes a cryptographic combiner (which could be an encryption combiner as claimed in dependent claim 10 or a decryption combiner as claimed in dependent claim 11) in a stream cipher cryptosystem. Independent claim 18 claims a method of encrypting a plaintext binary

data sequence. Independent claim 31 claims a method of decrypting a ciphertext binary data sequence.

The Ritter patent does not teach or suggestion cryptographically combining a first binary data sequence and the keystream and **performing two sequential non-associative operations** on the first binary data sequence and the keystream to provide a second binary data sequence as included in the limitations of independent claims 1, 9, 18, and 31.

By contrast, the Ritter patent discloses a dynamic substitution combiner and extractor. In the Ritter patent, a plaintext value on input 10 is transformed by substitution 12 into a ciphertext value output 14. A ciphertext value on input 22 is transformed by substitution 24 into the original plaintext value on output 26. Substitution 12 must be invertible to make this work. For example, the substitution table in substitution 12 can be made exactly as large as the number of possible input values 10 and filled sequentially with the possible output values. If no output value appears more than once, substitution 12 will be invertible. Substitution 12 can then be shuffled or randomized in any number of ways, as long as the values in the table in substitution 12 are re-arranged or permuted, substitution 12 will remain invertible. Typically, substitution 12 is implemented as addressable storage and realized with an electronic memory device, or an addressable area of memory hardware in an electronic digital computer or microprocessor. The substitution changes controller 18 uses both substitution input 10 and combiner substitution changes input 16 to change the content of substitution 12 by way of combiner substitution changes controls 20.

Thus, the Ritter patent dynamic substitution combiner and extractor device is similar to the very complex cryptographic combiner discussed in the Background of Invention section of the present application. As stated in the Background of Invention section of the present application, one example cryptographic combiner in this very complex category is a permutation table combiner, wherein the permutation table is required to have a table the size of the plaintext alphabet. By contrast, each two sequential non-associative operations according to claims 1, 9, 18, and 31 can be implemented with substantially the same complexity as the XOR and other linear combiner operations. As stated in the present application at page 12, lines 14-17, since each combiner operation according to the present invention is substantially the same complexity

as the XOR and other linear combiner operations, there is not the extensive expense in time, hardware and/or software resources of conventional very complex combiner operations (such as the dynamic substitution combiner extractor disclosed in the Ritter patent).

Moreover, the Ritter patent actually teaches away from the present invention, as the Ritter patent, at column 3, lines 7-9 states that the "alternative of selecting some other simple Boolean logic function to replace the exclusive-OR combiner does not work." In the Final Office Action the Examiner states that the Ritter patent teaches an improvement upon exclusive-OR at columns 3, lines 23-62. The Examiner recited text of the Ritter patent, however, actually teaches away from the present invention in further detail to the above-recited text at column 3, lines 7-9. For example, in summarizing its discussion of the background U.S. Patent No. 4,195,196 prior art, the Ritter patent at column 3, lines 55-59 states that the 4,195,196 mechanism is an example of a pseudo-random confusion generator plus conventional exclusive-OR combining, and is "thus susceptible to the plaintext attack, which is a weakness of all exclusive-OR combiners." Thus, the Ritter patent teaches away from a system or method of cryptographic combining such as claimed in independent claims 1, 9, 18, and 31 which can be implemented with two sequential non-associative operations having substantially the same complexity as the XOR and other linear operations. Instead, the Ritter patent, solves the problem of the susceptibility of the plaintext attack for exclusive-OR combiners with a dynamic substitution combiner and extractor device which is a very complex cryptographic combiner.

By contrast, the cryptographically combining a first binary data sequence in keystream and performing two sequential non-associative operations on the first binary data sequence and the keystream to provide a second binary data sequence as recited in independent claims 1, 9, 18, and 31 can solve problems of conventional XOR and other linear combiner operations used in cryptosystems, such as having known plaintext being combined with associated ciphertext to reveal the keystream; accidental double encryption to remove the keystream from the combined output bits; or combining two ciphertexts to eliminate the keystream and leaving a combination of the two original plaintext messages. Nonetheless, the stream cipher cryptosystems and methods of independent claims 1, 9, 18, and 31 can be implemented with a minimal increase of

resources over conventional XOR and other linear combiner operations as compared to the very complex solution to this problem proposed in the Ritter patent.

In view of the above, Appellant respectfully submits that independent claims 1,9, 18, and 31 are patentably distinct over the Ritter patent, because the Ritter patent does not teach or suggest the stream cipher cryptosystems of independent claims 1 and 9, the method of encrypting of independent claim 18, or the method of decrypting of independent claim 31. In addition, dependent claims 2-8 further define patentably distinct independent claim 1, dependent claims 10-17 further define patentably distinct independent claim 9, dependent claims 19-30 further define patentably distinct independent 18, and dependent claims 32-43 further define patentably distinct independent claim 31. Therefore, these dependent claims are also believed to be patentably distinct over the Ritter patent.

For the above reasons, Appellant respectfully requests reversal of the Examiner's rejections to claims 1-43 under 35 U.S.C. § 102(b) based on the Ritter patent.

CONCLUSION

Claims 1-43 of the pending application stand twice rejected. Claims 1-43 are pending in their original form and recite limitations that are not taught or suggested by the Ritter patent.

In view of the above, Appellant respectfully submits that pending claims 1-43 are in form for allowance and are not taught or suggested by the cited references. Since, the pending claims patentably distinguish over the cited references, Appellant respectfully submits that the rejections must be withdrawn, and respectfully request the Examiner be reversed and claims 1-43 allowed.

Any inquiry regarding this Amendment and Response should be directed to either Patrick G. Billig at the below-listed telephone numbers or Kris T. Fredrick at Telephone No. (763) 954-5388. In addition, all correspondence should continue to be directed to the following address:

HONEYWELL INTERNATIONAL, INC.
Law Department AB2
P.O. Box 2245
Morristown, New Jersey 07962-9806

Respectfully submitted,

Kevin R. Driscoll,

By his attorneys,

DICKE, BILLIG & CZAJA, PLLC
Fifth Street Towers, Suite 2250
100 South Fifth Street
Minneapolis, MN 55402
Telephone: (612) 573-2003
Facsimile: (612) 573-2005

Dated: 9-1-05

PGB:cmj

Patrick G. Billig
Reg. No. 38,080

CERTIFICATE UNDER 37 C.F.R. 1.8:

The undersigned hereby certifies that this paper or papers, as described herein, are being deposited in the United States Postal Service, as first class mail, in an envelope address to: Mail Stop Appeal Brief – Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on this 1 day of September, 2005.

By
Name: Patrick G. Billig

CLAIMS APPENDIX

1. (Original) A stream cipher cryptosystem comprising:

a source for providing an encryption keystream;

an encryption combiner receiving a first plaintext binary data sequence and the encryption keystream and performing a first set of two non-associative operations on the first plaintext binary data sequence and the encryption keystream to provide a ciphertext binary data sequence;

a source for providing a decryption keystream; and

a decryption combiner receiving the ciphertext binary data sequence and the decryption keystream and performing a second set of two non-associative operations on the ciphertext binary data sequence and the decryption keystream to provide a second plaintext binary data sequence substantially similar to the first plaintext binary data sequence.

2. (Original) The stream cipher cryptosystem of claim 1 wherein each operation in the second set is the inverse of an operation in the first set.

3. (Original) The stream cipher cryptosystem of claim 1 wherein the operations in the first set include an integer addition operation and an XOR operation, and the operations in the second set include an integer subtraction operation and an XOR operation.

4. (Original) The stream cipher cryptosystem of claim 1 wherein the operations in the first set include an integer subtraction operation and an XOR operation, and the operations in the second set include an integer addition operation and an XOR operation.

5. (Original) The stream cipher cryptosystem of claim 1 wherein the operations in the first set include a modular multiplication operation and an XOR operation, and the operations in the second set include an inverse modular multiplication operation and an XOR operation.

6. (Original) The stream cipher cryptosystem of claim 1 wherein the operations in the first set include an inverse modular multiplication operation and an XOR operation, and the operations in the second set include a modular multiplication operation and an XOR operation.

7. (Original) The stream cipher cryptosystem of claim 1 wherein the operations in the first set include a rotate right operation and an XOR operation, and the operations in the second set include a rotate left operation and an XOR operation.

8. (Original) The stream cipher cryptosystem of claim 1 wherein the operations in the first set include a rotate left operation and an XOR operation, and the operations in the second set include a rotate right operation and an XOR operation.

9. (Original) A stream cipher cryptosystem comprising:

a source for receiving a key and providing a keystream; and

a cryptographic combiner receiving a first binary data sequence and the keystream and performing two sequential non-associative operations on the first binary data sequence and the keystream to provide a second binary data sequence.

10. (Original) The stream cipher cryptosystem of claim 9 wherein the cryptographic combiner is an encryption combiner and the first binary data sequence is a plaintext binary data sequence and the second binary data sequence is a ciphertext binary data sequence.

11. (Original) The stream cipher cryptosystem of claim 9 wherein the cryptographic combiner is a decryption combiner and the first binary data sequence is a ciphertext binary data sequence and the second binary data sequence is a plaintext binary data sequence.

12. (Original) The stream cipher cryptosystem of claim 9 wherein the two sequential non-associative operations are an integer addition operation and an XOR operation.

13. (Original) The stream cipher cryptosystem of claim 9 wherein the two sequential non-associative operations are an integer subtraction operation and an XOR operation.

14. (Original) The stream cipher cryptosystem of claim 9 wherein the two sequential non-associative operations are a modular multiplication operation and an XOR operation.

15. (Original) The stream cipher cryptosystem of claim 9 wherein the two sequential non-associative operations are an inverse modular multiplication operation and an XOR operation.

16. (Original) The stream cipher cryptosystem of claim 9 wherein the two sequential non-associative operations are a rotate right operation and an XOR operation.

17. (Original) The stream cipher cryptosystem of claim 9 wherein the two sequential non-associative operations are a rotate left operation and an XOR operation.

18. (Original) A method of encrypting a plaintext binary data sequence, the method comprising the steps of:

generating an encryption keystream as a function of a key; and

combining the plaintext binary data sequence and the encryption keystream with two non-associative operations to provide a ciphertext binary data sequence.

19. (Original) The method of claim 18 wherein the two non-associative operations include an integer addition operation.

20. (Original) The method of claim 19 wherein the two non-associative operations include an XOR operation.

21. (Original) The method of claim 18 wherein the two non-associative operations include an integer subtraction operation.

22. (Original) The method of claim 21 wherein the two non-associative operations include an XOR operation.

23. (Original) The method of claim 18 wherein the two non-associative operations include a modular multiplication operation.

24. (Original) The method of claim 23 wherein the two non-associative operations include an XOR operation.

25. (Original) The method of claim 18 wherein the two non-associative operations include an inverse modular multiplication operation.

26. (Original) The method of claim 25 wherein the two non-associative operations include an XOR operation.

27. (Original) The method of claim 18 wherein the two non-associative operations include a rotate right operation.

28. (Original) The method of claim 27 wherein the two non-associative operations include an XOR operation.

29. (Original) The method of claim 18 wherein the two non-associative operations include a rotate left operation.

30. (Original) The method of claim 29 wherein the two non-associative operations include an XOR operation.

31. (Original) A method of decrypting a ciphertext binary data sequence, the method comprising the steps of:

generating a decryption keystream as a function of a key; and

combining the ciphertext binary data sequence and the decryption keystream with two non-associative operations to provide a plaintext binary data sequence.

32. (Original) The method of claim 31 wherein the two non-associative operations include an integer addition operation.

33. (Original) The method of claim 32 wherein the two non-associative operations include an XOR operation.

34. (Original) The method of claim 31 wherein the two non-associative operations include an integer subtraction operation.

35. (Original) The method of claim 34 wherein the two non-associative operations include an XOR operation.

36. (Original) The method of claim 31 wherein the two non-associative operations include a modular multiplication operation.

37. (Original) The method of claim 36 wherein the two non-associative operations include an XOR operation.

38. (Original) The method of claim 31 wherein the two non-associative operations include an inverse modular multiplication operation.

39. (Original) The method of claim 38 wherein the two non-associative operations include an XOR operation.

40. (Original) The method of claim 31 wherein the two non-associative operations include a rotate right operation.

41. (Original) The method of claim 40 wherein the two non-associative operations include an XOR operation.

42. (Original) The method of claim 31 wherein the two non-associative operations include a rotate left operation.

43. (Original) The method of claim 42 wherein the two non-associative operations include an XOR operation.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.